

**PCSRF, AGA HQ, Washington, D.C.
August 21, 2002**

Secure Multi-hop Peer-to-Peer Wireless Network/Pilot Test

William J. Miller
President
Maximum Control Technologies
a MILLER W J & ASSOCIATES Company

mact-usa@att.net

Aug. 21, 2002
Unclassified

Outline

- Motivation
- Requirements
- Pilot Test Overview
- Pilot Goals
- Technology Background
 - IEEE 802.11a and 802.11b
 - Signal Propagation Issues
 - 802.11 Features
 - Infrastructure Mode
 - Ad-hoc Mode (basis for Multi-hop)
 - Interference
- Wave Relay™
 - Multi-hop Operation
 - Secure Channel
- Security Comparison of WEP and Wave Relay™
- Other issues
 - Multi-hop Bandwidth Reduction
 - Speed Locking Option
- Industrial Plant Network (Wired and Wireless)
- Conclusions

Motivation

- Increase productivity
- Protection of assets
- Reduce costs
- Flexibility
- Convenience

Requirements

- Security safeguard must not impact performance or compromise operations
- Install with minimum downtime or while in operation
- Provide end-to-end security for wireless/wired nodes
- Must be easy to implement and use

Pilot Test Overview

- Test the operability of currently available wireless technology in an industrial plant
- No wired network infrastructure throughout the plant or in surrounding areas
- The environment has a number of obstacles including steel grating, sheet metal, and steel beams which may effect on wireless signal propagation.
- To evaluate it use under a range of environmental conditions including dust, extreme temperature and intermittent power conditions
- To use the devices in the performance of operations and maintenance functions by plant personnel

Pilot Goals

- Feasibility testing of current wireless radio technology
 - 802.11b (PC Card and USB Adaptor form factors)
 - 802.11a (PC Card form factor)
 - 2.4 Ghz external antennas (Omni and Yagi types)
- Wave Relay™ feasibility testing:
 - OS Integration
 - Multiple hop operation
 - Security
 - Embedded Implementation
- Remote monitoring and control testing:
 - pcAnywhere V10.5.1

Technology Background

Comparison of 802.11 standards

IEEE Standard	802.11b	802.11a
MAC Protocol	CSMA/CA	CSMA/CA
Modulation Scheme	DSSS	OFDM
Frequency Band (GHz)	2.4 -2.48	5.15 - 5.35
Independent Channels	3	8
Base Band Speeds (Mbits)	1, 2, 5.5, 11	6, 9, 12, 18, 24, 36, 48, 54
Peak Real Throughput (Mbits)	6	30

Signal Propagation Issues

- 802.11 cards support a range of speeds to provide flexibility in a variety of operating conditions
- The speed selection is determined by modulation schemes each of which has a different level of noise immunity
- The most appropriate speed is chosen based on the signal strength and noise characteristics of the wireless medium
- The result is that devices that are right next to each other will communicate at the fastest speed. As they move farther away, or obstruction are encountered, the speed will shift to a slower speed

Signal Propagation Issues (Cont.)

- *Dense obstacles absorb the wireless signal and metal such as steel tend to reflect the signal.*
- *Reflections can cause a condition referred to as “Multi-path fading” which is a result of the time differential between signals that either cause the signal to sum or cancel depending on the phase shift.*
- *Theory indicates that the 802.11a (OFDM) modulation scheme should perform better in a multi-path environment than the 802.11b (DSSS) modulation scheme*

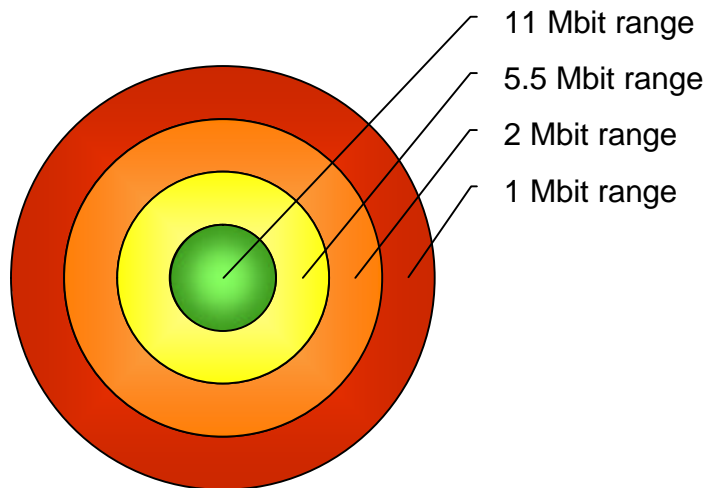
Signal Propagation Issues (Cont.)

- *To boost signal strength, and thus speed is obtained through*
 - *the use of a bi-directional amplifier to increase transmit power and receiver input sensitivity,*
 - *the use of a direction antenna*

Comparison of Antenna Type

Antenna Type	Horizontal Coverage	Vertical Coverage	Typical Gain (dB)
Dipole	360	90-180	0-3
Omni	360	5-20	6-15
Sector	90-180	5-20	10-25
Parabolic	5-20	5-20	15-30
Yagi	30-45	30-45	10-15
Patch	30-90	30-90	5-15

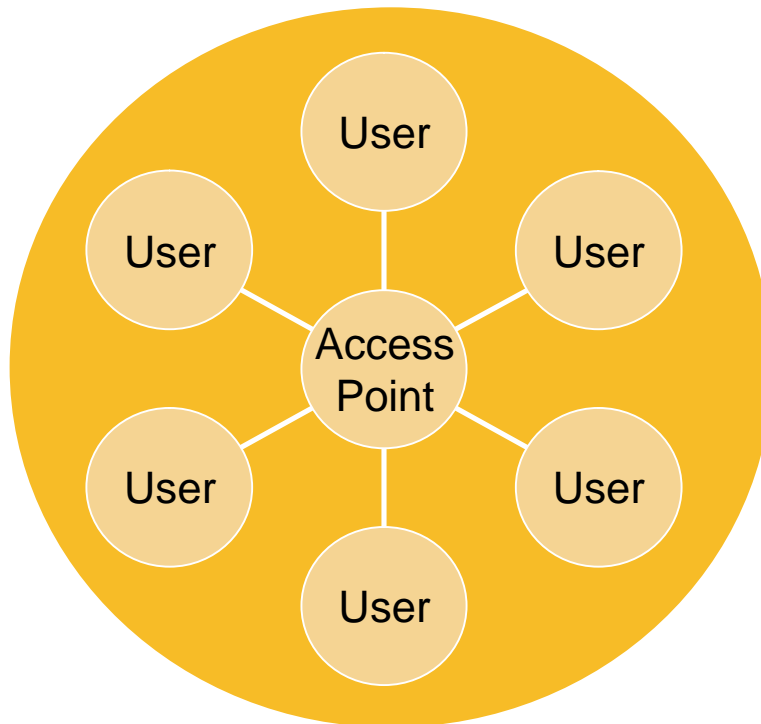
802.11 Features



- IEEE wireless networking standard
- Multiple data rates support different ranges
- Unicast, Multicast, and Broadcast services
- WEP hardware encryption
 - Static shared key
 - Stream cipher
 - Exploitable
- Two modes of operation
 - Infrastructure
 - Ad hoc

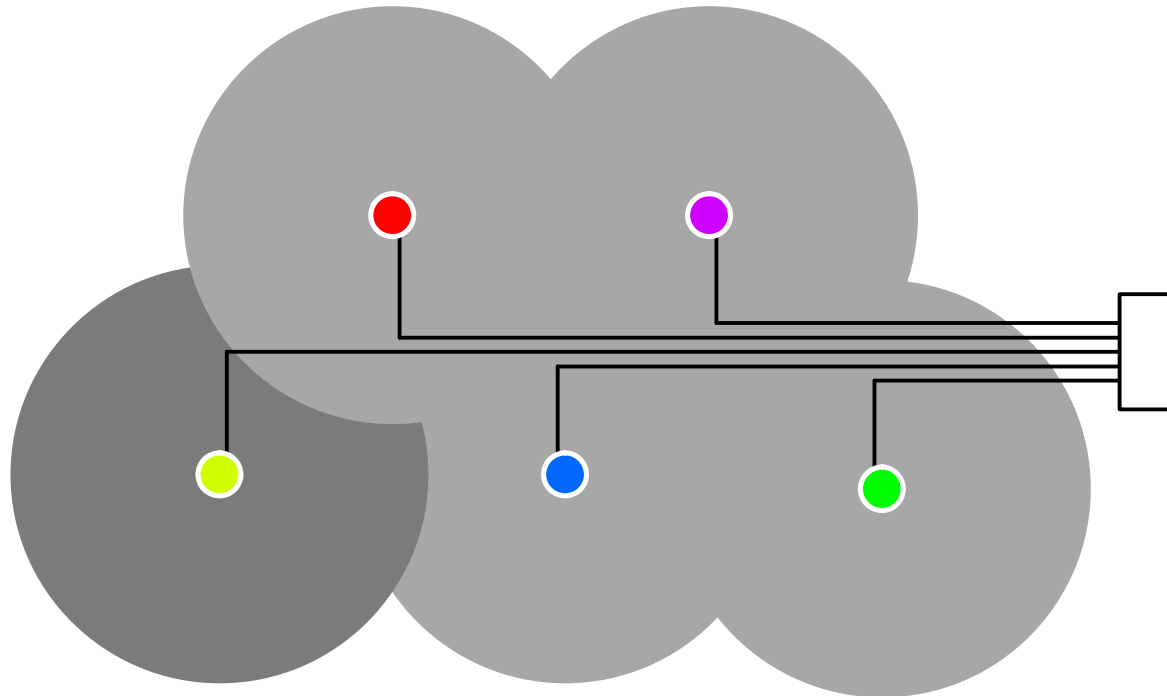
802.11 Infrastructure Mode

- Access Point centric network
- Patterned after traditional client-server model



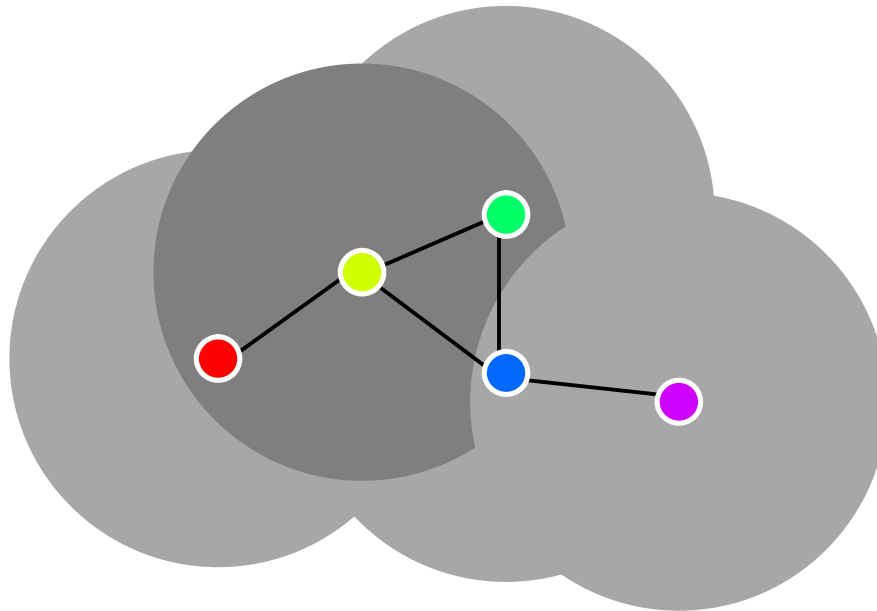
802.11 Access Points

- Require a connection to the wired network
- Adding users burdens the infrastructure with no benefit
- Requires centralized authentication
- Fixed Network topology



802.11 Ad-hoc Mode (basis for multi-hop)

- Infrastructure formed by the cooperation of network nodes
- Adding users results in more infrastructure and increased connectivity
- Redundant data paths provide fault tolerance
- Extended range for users
- Dynamic Network topology



802.11 Interference

- The 2.4-2.48 Ghz band used by 802.11b has some potential of interference and the new 5.15-5.35 Ghz band used by 802.11a has none at present
- Potential sources of interference:
 - 2.4 Ghz portable phones
 - Microwave ovens
 - Bluetooth devices

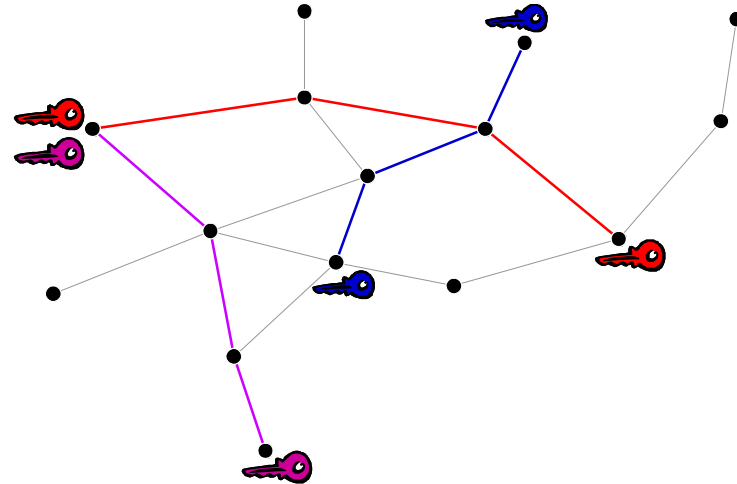
Wave Relay™ - A Secure Channel Solution

- **Secure Channel**

- Established on-demand
- Robust key exchange protocol that establishes pair-wise secret shared keys
- Shared key used for AES or Blowfish block cipher encryption and SHA1 hash
- Multiple connections between two nodes share the same secure channel
- End-to-end security model that can include both wireless and wired nodes

- **Public Key Infrastructure (PKI)**

- Each node has a private key
- Public keys are X.509 certificates that are signed by a Certificate Authority (CA)
- Certificates of other nodes may be pre-stored, retrieved from an available CA, or traded as part of the exchange
- Certificate revocation via direct communication with the CA or by CA signed revocation lists propagated through the network



- **Key Exchange**

- Authentication provided by the PKI
- Shared key provided by Diffie-Hellman exchange
- Robust against network losses
- Immunity against replay attacks by using a double challenge & response
- Automatic key refresh based on time and quantity of data transferred

*Wave Relay*TM - Attack Avoidance

- Addressed Attacks
 - Impersonation, Man-in-the-Middle, and Replay
 - Prevented by the authenticated key exchange protocol
 - Over-hearing, Fabrication, or Modification of packets
 - Prevented by encryption and hash verification
 - Session Hijacking
 - Impossible because of the pair-wise secret keys
- Future Addressed Attacks
 - Byzantine Routing Failures
 - Caused by either a malicious or corrupt authenticated node
 - Addressed by a secure routing protocol
 - Protocol must do more than just authenticate nodes
 - Must detect and avoid faults

Security Comparison of *WEP* and *Wave Relay*TM

Brief Security Comparison of *WEP* and *Wave Relay*TM

	<i>WEP</i>	<i>Wave Relay</i> TM
Key Type	Shared Key	Pair-wise Keys
Key Creation	Static	Periodic Exchange
Authentication	Shared Key	PKI
Encryption	Stream Cipher	Block Cipher

Other Issues

- Multi-hop Bandwidth Reduction
 - While multiple hops allow greater extension and reliability through redundant path, they come at the cost of bandwidth
 - Two neighboring nodes cannot transmit at the same time
 - This is a common property of all broadcast networks including unswitched Ethernet
 - The bandwidth reduction is effectively halves the bandwidth per hop until the node that is no longer in range
 - The end result is that the bandwidth is $1/2$ to $1/8$ the original speed in extreme cases.
 - Internet access is not noticeably affected because the reduced bandwidth is capable of saturating most internet connections

Other Issues (Cont.)

- Speed Locking Option
 - Performance can be increased by locking the operating speed of the wireless cards to 5.5 or 11 Megabits
 - High speed guarantees that the shared medium is efficiently used
 - The main downside is that the range is reduced
 - Disabling the wireless card's ability to choose different speeds is only recommended for networks where higher bandwidth is worth the extra cost and reduced flexibility

Industrial Plant Network (Wired)



- This diagram has been remove since it may contain sensitive information related to homeland security

Industrial Plant Network (Wireless)



- This diagram has been remove since it may contain sensitive information related to homeland security

Conclusions

- *Wave Relay™ self-configuring network was able to move data across multiple hops*
- *802.11a was unable to deliver and failed to provide connectivity in the industrial environment*
- *Wave Relay™ provided always-on end-to-end security for access to mission critical computing assets*
- *Intermediate multi-hop devices facilitates rapid deployment at reduced cost*
- *The use of 802.11 would provide more flexible operations and maintenance capabilities*
- *The installation of Wave Relay Routers™ to serve as fixed intermediate nodes will provide fault tolerance through multi-path redundancy*

Conclusions (Cont.)

- *802.11 networks*
 - *Can be made secure
and provides greater mobility
and fault tolerance*
- *Adversaries of MP2P WLAN's*
 - *Need to be more technically sophisticated*
- *Multi-hop p2p wireless networks
can provide protection for
mission critical assets*